To Design, Implement and Test advanced cryptographic algorithm for enhancing security

1. Introduction:

Computer technology is more and more ubiquitous; the penetration of computer in society is a welcome step towards modernization but society needs to be better equipped to grapple with challenges associated with technology. Data security has become crucial aspect now a days in every sectors. So in order to protect it various methods and algorithms have been implemented cryptography combines mathematics, computer science (software, hardware), engineering and networking. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered and create difficulty for the security professionals in order to catch hackers. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information.

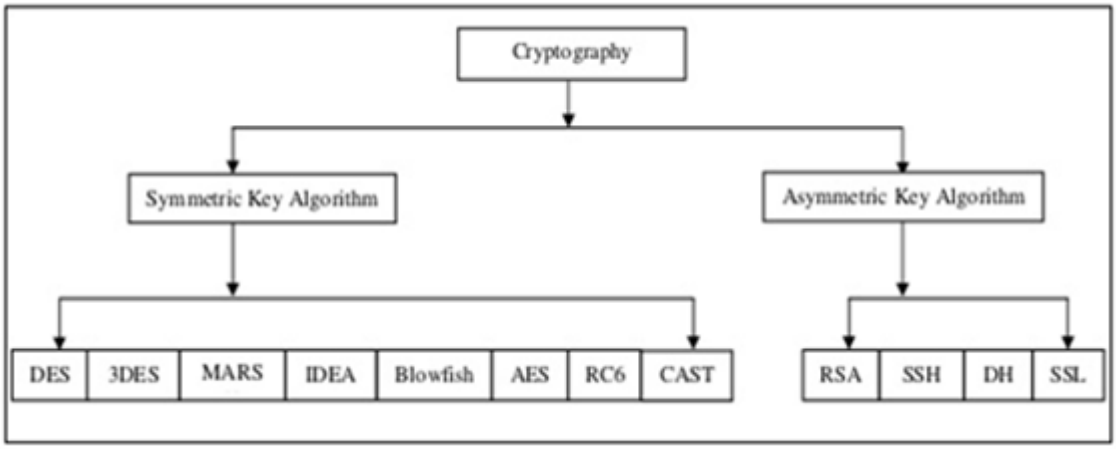
The recent research is focused on bringing quality security training combined with rapidly changing technology. Online networking security is to provide a solid understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures. Many businesses are critically reliant on their information systems for key business processes (e.g. websites, production scheduling, transaction processing), security can be seen to be a very important area for management to get right. Importance features of security are confidentiality, authentication, integrity, non repudiation identification.

These days the applications like Internet and networks are growing very fast, thereby the importance and the value of the exchanged data over the internet or other media types are increasing. For secure communication the cryptography is essential in information security, Cryptography algorithms is very important.

A **cipher**, or **cryptographic algorithm**, is the means of altering data from a readable form (also known as plaintext) to a protected form (also known as cipher text), and back to the readable form. Changing plaintext to cipher text is known as **encryption**, whereas changing cipher text to plaintext is known as decryption. [22]

A cryptographic algorithms is (also called encryption algorithms) a "mathematical algorithm, used in conjunction with a secret key, that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm. Such algorithms are also the basis for digital signatures and key exchange."[23]

There are several ways of classifying cryptographic algorithms.



As a researcher I would like to intended, test and implement a modified algorithm to get rid of the current threats in security like viruses, worms etc.Then this purposed work will also be implemented to get the algorithm to resolve the related issues. The purposed algorithm will be tested and then implemented.

2. Review of Literature and Development in the Subject:

The following section reveals the review of literature on the above mentioned area of research:

- According to Christopher Leidigh(2005), Director of Communication and Technology Research with APC, with the increased number of threats to networks such as worms, viruses and clever hackers, security can no longer be viewed as an option, even within "private" networks. Securing all equipment, including physical infrastructure equipment such as UPS systems and HVAC systems, is critical to maintaining uptime and seamless access to services. Providing and maintaining security across the enterprise typically means increased administration. Historically, this has been the largest barrier to broad implementations of security. Today, the amount of time spent repairing a network due to just a single worm or virus attack can easily be greater than the upfront time to more adequately secure an enterprise. Fortunately, there are many options in systems and software to increase the security of the network while reducing the overhead of managing such systems. Even basic practices such as periodic software updates, locking down all devices and using centralized authentication and secure access methods can go a long way to reducing risks. Institution of appropriate security policies and frequent network audits further increase the overall protection of the network.[2]

- Lambert Schaelicke (2008) Network explained that intrusion detection systems (NIDS) are becoming an important tool for protecting critical information and infrastructure. The quality of a NIDS is described by the percentage of true attacks detected combined with the number of false alerts. However, even a high-quality NIDS algorithm is not effective if its processing cost is too high, since the resulting loss of packets increases the probability that an attack is not detected. This study measures and compares two major components of the NIDS processing cost on a number of diverse systems to pinpoint performance bottlenecks and to determine the impact of operating system and architecture differences. Results show that even on moderate-speed networks, many systems are inadequate as NIDS platforms. Performance depends not only on the processor performance, but to a large extent also on the memory system. Recent

trends in processor micro architecture towards deep pipelines have a negative impact on the systems NIDS capabilities, and multiprocessor architectures usually do not lead to significant performance improvements. Overall, these results provide valuable guidelines for NIDS developers and adopters for choosing a suitable platform, and highlight the need to consider processing cost when developing and evaluating NIDS techniques.[5]

- Prof T Ramanujan and Ram Kumar Singh (2009), has described some of the previous efforts to measure IDS, and have outlined some of the difficulties that have been encountered. However, because both normal and attack traffic are so variable from site to site, and because normal and attack traffic evolve over time Solving the problem of high availability and security simultaneously offers the opportunity for more reliability than systems which solve the problems separately, in addition to being easier to implement, and offering increased opportunity for recording and data analysis. The integration of these two technologies, however, is a non-trivial task. A fine balance must be achieved between speed and robustness of IDS features – it is equally bad to have the web server crash because an attack was missed, or drop large amounts of traffic due to an overly through IDS becoming a bottleneck. Additionally, while a content-based load balancer offers many advantages over separate Load Balancing and IDS solutions, it also suffers from the drawbacks of both. It has been said that the three things most important to a server manger are Security (the ability to withstand hacking), High-Availability (the ability to withstand hardware failure), and low-latency (the ability to service requests quickly). With the current implementation of secure direct, the first two criteria, security and high availability, are satisfied. In regards to latency, our experiments have (once again) shown that there is a trade-off between security and performance. While improving the efficiency of the programming can mitigate this problem to an extent, the trade-off is certain to remain, and choosing the right balance will likely continue to be a difficult task for the system administrator. It is the authors' opinion that this type of system could provide a much needed additional security tool, however, a good deal of streamlining work remains before it could be widely deployed.[1]

- M.Sadiq Ali Khan(2010) As OS drivers have more efficiency with less audit feature for attack detection and less protectibility for system calls. Whilst host-based intrusion detection systems work well for deployment on smaller numbers of systems i.e. the tracking, monitoring and maintaining of hundreds or thousands of systems can quickly become a cumbersome overhead in terms of costs and resources. Proposed model makes it possible to justify the selection of the method for building a data acquisition module of host-based IDS.[4]

- Amrita Anand (2012) says that before determining a network traffic is a potential threat to a network or not, there is a need for IDS to have a method in differentiating whether it is malicious or not. Therefore, this research has introduced a new methodology to identify a fast attack intrusion using time based detection. The method used to identifies anomalies based on the number of connection made in 1 second. For further validation, the methodology will be implemented on a different set of real network traffic. In view of the fact that this research only concentrate on the TCP connection only, in the near future the researcher are planning to investigate use other protocol and other flag to recognize the fast attack intrusion activity. Inspecting other protocol and flag it may help to detect fast attack intrusion activities that launch using UDP or ICMP protocol. Finally the approach introduce in this research will be implemented on a production network for accessing the performance on the anomalies detection using time based detection.[3]

- Harsh Mathur, Prof.Zahid Alam (2015), comparative study between IDEA,RSA and AES are carried out into nine factors, which are key length, cipher type, block size, developed cryptology analysis resistance,security,possibility key, possible acsii printable character keys, time required to check all possible key at 50 billion second, these factors proved the AES is better than IDEA and RSA an important application oriented problem concerning the data security has been presented. The author hopes that this work may have some influence on the future standardization policy in encryption and decryption.[6]

- Ali M Alshahrani and Prof. Stuart Walker (2015), a novel cubic symmetric block cipher technique is discussed. The greatest advantages of this technique are the length of the key, the technique used to generate the key, and that the suggested algorithm and tools are very lightweight and so are inexpensive. Moreover, the algorithm can be used with all different kinds of data because it will not cause any specific delay. Two keys are used to produce this strong algorithm. The first one is a shared key that will be used to scramble the home keys to get the key that will be XoR-ed with the plain text. Compared to the AES, less time is required to encrypt and decrypt the tested message. However, the delay will be affected by the number of rounds that will be used to generate the key so it is highly recommended
that fewer rounds be used.[25]

3. Objective of Research / Proposed Hypothesis:

The main purpose of the research is to learn the tools and motives involved in computer and network attacks. There is a commitment to moving far beyond theory and providing solid information about common threats.

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether someone attempted to break into your system, if they were successful, and what they may have done.

In this proposed work I will be studying the various cryptography algorithms and security tools which already exist till date of submission of my synopses. In this purpose work designing, implementing and testing of the new (proposed) algorithm will be exercised using suitable security tools, simulated in software like (mat lab or any other simulator) for the chosen research parameter. And this new proposed algorithm will be implemented using java or vb.net to get the better security of the information and implementation. Since entire universal is a sharing lot of information justifies the need of better information security system very well.

General limitations of cryptographic algorithm emphasizes on the selection between hardware & software cryptosystem. & limitation transparent for application.

My proposed research work is to develop a innovative algorithm which will overcome the shortcomings of following algorithm.

parameter / Algorithms	Structure	Development	Key length (Bits)	Block of size	No. of rounds	Attack found	Flexibility	Remarks	Conclusion
DES (Data Encryption Algorithms)	Fiestel	1970s at IBM& published by 1977.	64 bit (56 bit usable)	64	16	Brute force	No	DES is encryption scheme, especially in financial applications	It is exposed to Brute force attack because of the weak keys.
3DES (Data Encryption Algorithms)	Fiestel	published in 1998	168	64	48	Brute force, chosen plain text	Yes	In 3DES memory required for implementation is the highest means it is the slowest algorithm	3DES is easy to implement (and accelerate) in both hardware and software
CAST-128	Fiestel	Carlisle Adams and Stafford Tavares	40 to 128	64	12 to 16	The resistance against both linear & differential attack	Yes	available worldwide on a royalty-free basis for commercial and non-commercial uses	it has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule
BLOWFISH	Fiestel	*Bruce Schneier by 1994*	32-448	64	16	Timing attack or infeasible	Yes	It suffers from weak key problem	Reliability of blowfish is questionable due to the large number of weak keys.
IDEA (International Data Encryption Algorithm)	Substitution permutation network	Xuejia Lai and James Massey, in 1992	128	64	8.5	Key schedule attack	No	Idea is exposed to collision attack.	Resistant to both linear & differential analysis.
AES (Advanced Encryption Standard)	Substitution permutation network	Dr. Joan Daemen and Dr. Vincent Rijmen in oct 2000.	256,192 or 128	128	14,12 or 10	Side channel attack	Yes	Related key attackers can clearly be avoided by always	It has no serious weakness although it was observed

								selecting cryptographic key independtly at random	that a mathematical property of the cipher might be vulnerable into an attack. It can break different related key
RC6 (Rivest Cipher 6)	Fiestel	Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin	256,192 or 128	128	20	Highly resistant to differential & cryptanalical attack	Yes	RC6 is vulnerable to differential brute force attack if the key size is small.	Time consumption for process in RC6 is high.
RSA	factorization	1977 by Ron Rivest, Adi Shamir and Leonard Adleman	1024-4096	variable	Not applicable	Timing attack	Yes	Cryptosystem based on factoring are actually usually based not on the difficulty of solving RSA problem	Using small & relatively close primes. Primes are small enough then factorizing close then, finding out the common factors reveals the public key. It consumes longest encryption time & memory usage which ultimately slow down the speed of the algorithms.

Table 1.0 Analysis of Parameters for Cryptography

I have analyzed various encryption algorithms. I found that each algorithm has it's possess benefits according to different parameters. Algorithm depends upon the key management, type of cryptography, number of keys, number of bits, number of rounds, limitations used in a key. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data.

I studied the various cryptographic algorithms and majorly deals the encryption and decryption process for protecting the text files and images using some of the cryptographic algorithms.

Finally by analyzing Encryption/Decryption time, Encryption/Decryption Throughput and Power Consumption value in future, there is wide scope of improvement in these both encryption. I have analyzed all algorithms in the above given table and in future I will select one of them & implement new one.

4. Proposed Work Plan / Formulation and Structure Study:

For the above Research Work, we need design a scheduler to complete the research work,

1) First Six Months I will study the all the previous work on my topic.
2) In Next Eight Months I will collect the information or data which is related to my research.
3) In Next Eight Months I will design an algorithm and I will implements it as a part of my research work and will carry out for the testing of the algorithm selected parameters.
4) In next five months I will be writing the chapters related to my complete thesis.
5) Then finally thesis will be submitted after pre viva.

5. References:

[1] International Journal of computer science and information security vol.2 No.1,2009.[IJCSIS]

[2] www.apc.com, riv 2005

[3] Amrita et al, International journal of advanced research in computer science and software engineering 2[8], Aug, 2012.pp 94-98.

[4] Journal of Telecommunications, volume 2, issue 1, April 2010.

[5] www.onesearch.id.com

[6] Harsh Mathur, Prof.Zahid Alam, International Journal emerging Trends and Technology in computer science (IJETTCS) www.ijettcs.org. vol 4,issue 1, jan-feb 2015

[7] Cryptography and Network Security (Sie) By B. A. Forouzan Tata McGraw-Hill Education, Special Indian Edition 2007.

[8] Simon Edwards "Network Intrusion Detection Systems: Important IDS Network Security Vulnerabilities Must Know Information on Realizing and Overcoming the Risks" Whitepaper September 2012 http: //www.forum-intrusion.com/archive/ IDSB White Paper a141002.pdf

[9] K.Kalaiselvi, Anand Kumar International Journal of computer application(ICCTAC-2015)

[10] Shailja kumara,Jyoti Chawla International Journal of Innovation & advancement in computer science vol 4,issue may 2015

[11] M. Sabhnani and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context," Proc. International Conf. Machine Learning, Models, Technologies and Applications (MLMTA ',03), pp. 209-215, 2003.

[12] S.Pavitra, Mrs. E Ramadevi, International Journal of advanced research in computer Engineering & technology vol 1,issue 5 July 2012

[13] Mohammad Reza Ahmadi and DavoodMaleki, "An Intrusion Detection Technique using Co-Co Immune System for Distributed Data Networks (CoCo -ISD)" International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[14] O.B.Lawal "NETWORK SECURITY USING INTRUSION DETECTION & PREVENTION SYSTEM INTEGRATION MODEL", Computing, Information Systems, Development Informatics & Allied Research Journal, Vol. 4. No. 3, 2013

[15] Rani et al.,International Journal of advanced research in computer science and S.E5(8) august -2015

[16] M.V.Ramana Murthy et al "Performance of the Network Intrusion Detection Systems", International Journal of Computer Science and Network Security, VOL.9 No.10, October 2009.

[17] Algorithms-key sies and parameter Report 2013 recommandations.pdf foxit reader 2.0

[18] R. Kabila "Network Based Intrusion Detection and Prevention Systems in IP-Level Security Protocols", International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering Vol: 2, No: 10, 2008.

[19] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, Feb. 2007.

[20] Haslum K., Abraham A. and Knapskog S., DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment, Third International Symposium on Information Assurance and Security, IEEE Computer Society press, USA, ISBN 0-7695-2876-7, pp. 183-188, 2007.

[21] Md.Asif Mushtaque, International Journal of Computer Science & engineering vol- 2(4)

[22] Cipher cryptography algorithms dictionary definition| cipher or --- www.yourdictionary.com/cipher -or-cryptography algorithm

[23] ↑ ITU, "Compendium of Approved ITU-T Security Definitions," at 14 (Feb. 2003 ed.)

[24] Salfner F. and Malek M., Using Hidden Semi-Markov Models for Effective Online Failure Prediction, 26th IEEE International Symposium on Reliable Distributed Systems, pp.161-174, 2007.

[25] Ali M Alshahrani and Prof. Stuart Walker, Computer Science and Electronic Engineering,

University of Essex, Wivenhoe Park, Colchester, Essex, UK, C04 3SQ, International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 1, February 2015

[26] Feng Li, Wang W., Zhu L. and Zhang Y., Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation, Journal of Network and Computer Applications, pp. 721-732, 2009.

[27] Mu C. P., Huang H. K. and Tian S. F., Online risk assessment of intrusion scenarios using DS evidence theory, In Proceedings of 13th European symposium on research in computer security a LNCS, Málaga, Spain, ISBN 978-3-540-88312-8 , pp. 35-48, 2008.

[28] Mu C. P, and Li Y., An intrusion response decision-making model based on hierarchical task network planning, Journal of expert systems with applications, 2009.

[29] N. Stakhanova, S. Basu and J. Wong, Taxonomy of Intrusion Response Systems, International Journal of Information and Computer Security. Vol. 1. No. 1/2, pp.169-184, Inderscience, 2007.

[30] **www.ijarcsse.com**

Signature **Signature**

Research scholar **Research supervisor/Guide/Co-guide**

From

Dr.G.N.Shinde

Dean, Faculty of science

SRTM University Nanded.